Author(s): Joaquim, R (Joaquim, Rui); Ribeiro, C (Ribeiro, Carlos); Ferreira, P (Ferreira, Paulo)

Editor(s): Chaum, D; Jakobsson, M; Rivest, RL; Ryan, PYA; Benaloh, J; Kutylowski, M; Adida, B

Title: Improving Remote Voting Security with Code Voting

Source: Towards Trustworthy Elections: New Directions in Electronic Voting, 6000: 310-329 2010

Book series title: Lecture Notes in Computer Science

Language: English

Document Type: Proceedings Paper

Conference Title: Workshop on Trustworthy Elections

Conference Date: AUG, 2001

Conference Location: Tomales Bay, CA

Author Keywords: Remote voting; Internet voting; vote manipulation; uncontrolled voting platform; insecure voting platform

KeyWords Plus: SCHEME

Abstract: One of the major problems that prevents the spread of elections with the possibility of remote voting over electronic networks, also called Internet Voting, is the use of unreliable client platforms, such as the voter's computer and the Internet infrastructure connecting it to the election server. A computer connected to the Internet is exposed to viruses, worms, Trojans, spyware, malware and other threats that can compromise the election's integrity. For instance, it is possible to write a virus that changes the voter's vote to a predetermined vote on election's day. Another possible attack is the creation of a fake election web site where the voter uses a malicious vote program on the web site that manipulates the voter's vote (phishing/pharming attack). Such attacks may not disturb the election protocol, therefore can remain undetected in the eyes of the election auditors. We propose the use of Code Voting to overcome insecurity of the client platform. Code Voting consists in creating a secure communication channel to communicate the voter's vote between the voter and a trusted component attached to the voter's computer. Consequently, no one controlling the voter's computer can change the his/her's vote. The trusted component can then process the vote according to a cryptographic voting protocol to enable cryptographic verification at the server's side.

Addresses: [Joaquim, Rui; Ribeiro, Carlos; Ferreira, Paulo] Univ Tecn Lisbon, ISEL, INESC ID, Lisbon, Portugal

E-mail Address: rjoaquim@cc.isel.ipl.pt; carlos.ribeiro@tagus.ist.utl.pt; paulo.ferreira@inesc-id.pt

Publisher: SPRINGER-VERLAG BERLIN

Publisher Address: HEIDELBERGER PLATZ 3, D-14197 BERLIN, GERMANY

ISSN: 0302-9743

ISBN: 978-3-642-12979-7

29-char Source Abbrev.: LECT NOTE COMPUT SCI

ISI Document Delivery No.: BPO91